日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　９月　４日

出願番号
Application Number: 特願２００２－２５９１９０

[ST.10/C]: [ＪＰ２００２－２５９１９０]

出願人
Applicant(s): 株式会社日立製作所

２００３年　２月１４日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３００７９６２

【書類名】　特許願

【整理番号】　HI020539

【提出日】　平成14年 9月 4日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 1/26

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　大島　訓

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　佐藤　雅英

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100071283

【弁理士】

【氏名又は名称】　一色　健輔

【選任した代理人】

【識別番号】　100084906

【弁理士】

【氏名又は名称】　原島　典孝

【選任した代理人】

【識別番号】　100098523

【弁理士】

【氏名又は名称】　黒川　恵

【選任した代理人】

【識別番号】　100112748

【弁理士】

【氏名又は名称】　吉田　浩二

【選任した代理人】

【識別番号】　100110009

【弁理士】

【氏名又は名称】　青木　康

【手数料の表示】

【予納台帳番号】　011785

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティに関する情報を更新する方法、クライアント、サーバ、及び管理端末

【特許請求の範囲】

【請求項１】　クライアントとサーバとがネットワークを通じて接続され、

前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、

前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新するステップを備えることを特徴とするセキュリティに関する情報を更新する方法。

【請求項２】　前記クライアントはローカルなディスク装置を有しないことを特徴とする請求項１に記載のセキュリティに関する情報を更新する方法。

【請求項３】　前記サーバは管理端末とネットワークを通じて接続され、

前記セキュリティ情報を更新するステップでは、前記管理端末が、前記セキュリティ情報を更新することを特徴とする請求項１に記載のセキュリティに関する情報を更新する方法。

【請求項４】　前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることを特徴とする請求項１に記載のセキュリティに関する情報を更新する方法。

【請求項５】　前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることを特徴とする請求項４に記載のセキュリティに関する情報を更新する方法。

【請求項６】　前記クライアントが前記セキュリティ情報を参照することを特徴とする請求項１に記載のセキュリティに関する情報を更新する方法。

【請求項７】　前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むことを特徴とする請求項６に記載のセキュリティに関する情報を更新する方法。

【請求項８】　サーバにネットワークを通じて接続するクライアントであって、

前記クライアントが管理する記憶装置を前記サーバに備え、

前記記憶装置には、前記セキュリティ情報が格納されており、前記セキュリティ情報は更新され、

前記セキュリティ情報を参照することを特徴とするクライアント。

【請求項９】　前記クライアントはローカルなディスク装置を有しないことを特徴とする請求項８に記載のクライアント。

【請求項１０】　前記サーバは管理端末とネットワークを通じて接続され、前記管理端末が、前記セキュリティ情報を更新することを特徴とする請求項８に記載のクライアント。

【請求項１１】　前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることを特徴とする請求項８に記載のクライアント。

【請求項１２】　前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることを特徴とする請求項１１に記載のクライアント。

【請求項１３】　前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むことを特徴とする請求項８に記載のクライアント。

【請求項１４】　クライアントとネットワークを通じて接続されるサーバであって、

前記クライアントによって管理される記憶装置を備え、

前記記憶装置には、前記セキュリティ情報が格納され、前記セキュリティ情報は更新されることを特徴とするサーバ。

【請求項１５】　前記クライアントはローカルなディスク装置を有しないことを特徴とする請求項１４に記載のサーバ。

【請求項１６】　前記サーバは管理端末とネットワークを通じて接続され、

前記管理端末が、前記セキュリティ情報を更新することを特徴とする請求項１４に記載のサーバ。

【請求項１７】　前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることを特徴とする請求項１４に記載のサーバ。

【請求項１８】　前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることを特徴とする請求項１７に記載のサーバ。

【請求項１９】　前記セキュリティ情報は、前記クライアントにより参照されることを特徴とする請求項１４に記載のサーバ。

【請求項２０】　前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むことを特徴とする請求項１９に記載のサーバ。

【請求項２１】　クライアントによって管理される記憶装置を備えたサーバとネットワークを通じて接続される管理端末であって、

前記サーバの前記記憶装置には、前記セキュリティ情報が格納されており、前記セキュリティ情報を更新することを特徴とする管理端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、セキュリティに関する情報を更新する方法、クライアント、サーバ、及び管理端末に関する。

【０００２】

【従来の技術】

ネットワークを介してサーバに接続されるクライアントは、図７に示すように、ＣＰＵ、メモリ、ネットワークインタフェース、及びハードディスク装置で構成されるストレージ（ローカルなディスク装置）を備えている。メモリには、ＯＳ（Operating System）、セキュリティソフトウエア及びアプリケーションプロ

グラムが展開される。ストレージには各種ファイルが記憶されている。これら各種ファイルとしては、ＯＳを構成するファイル群やポリシファイル群、及び、その他ファイル群である。その他ファイル群としては、セキュリティソフトウエア、アプリケーションプログラム、データファイル（適宜、単にファイルと称する）、及びファイルシステムが含まれる。このファイルシステムには、各ファイルの属性やファイルアロケーションテーブル等、様々なファイルの管理情報が記述されている（例えば、非特許文献１参照）。

【０００３】

一般的なＯＳの制御の下では、図８に示すように、アプリケーションプログラムがファイルに対してアクセスを要求すると（Ｓ１０）、ファイルアクセス制御機能によりファイルシステムが参照され、アクセスの可否が判定される（Ｓ２０）。この判定で許可されると、アプリケーションプログラムはドライバによりファイルにアクセスできる（Ｓ３０→Ｓ４０）。また、アプリケーションプログラムがアクセスするファイルは、ネットワークを介して接続されるサーバ側のファイルも含む。すなわち、ネットワークドライバ及びネットワークカードにより、ネットワークを介して接続されるサーバ側のファイルにアクセスする（Ｓ５０→Ｓ６０→Ｓ７０）。

【０００４】

このストレージに格納されるファイルシステムの内容としては、例えば、ファイル属性（図２参照、例えば、非特許文献２参照）、アロケーションテーブル（図３参照）、及びクラスタ（図４参照）がある。図２のファイル属性に示すように、各ファイルについて、ファイル名やパス名をはじめ、所有者やグループ名等の属性が対応づけられている。特に、所有者やグループ、及び外部といったユーザからの各ファイルへのアクセスに関し、読み出し（図中「読」）や書き込み（図中「書」）及び実行といった各項目を設けている。そして、これら各項目について、許可（図中「可」）や不許可（図中「不」）といったアクセス権に関する属性が対応づけられている。

【０００５】

そして、図７に示すセキュリティソフトウエアは、ＯＳに追加するソフトウエ

アであり、前述したアクセス制御機能を強化する。このセキュリティソフトウエアは、ポリシファイルに記述されたアクセス制御情報に基づき、よりセキュリティを高める緻密なアクセス制御を行う。このポリシファイルには、ファイルに対するアクセスを許可する条件として、ユーザやアプリケーション及び時間帯等の詳細な属性が特定されている。

【０００６】

また、このポリシファイルには、ウイルスパターンファイルや、シグネチャファイルも含まれる。ウイルスパターンファイルは、アンチウイルスソフトと称されるウイルス対策用ソフトウエアに用いられる。シグネチャファイルは、ホスト型侵入検知システムと称されるネットワーク攻撃対策用ソフトウエアに用いられる。アンチウイルスソフトは、コンピュータウイルスの特徴を示すパターンに基づき、ファイルのオープン時または一定期間毎に、ファイルに対するコンピュータウイルスの感染の有無を検査し、必要な処置を適宜に講じる。ホスト型侵入検知システムは、シグネチャと呼ばれるネットワークパケットを識別し、ネットワークを通じた攻撃を検知したり、実行中のアプリケーションプログラムが出力したログファイル等を監視し、攻撃を検知する。

【０００７】

ここで、ポリシ（セキュリティポリシ）とは、コンピュータの使用に関する制限を総称したセキュリティ情報である。つまり、ポリシとは、特定のアプリケーションの実行を禁止したり、設定変更を防止するための情報だけでなく、各種ソフトウエアも含む。

【０００８】

次に、ネットワーク環境下におけるポリシファイルの更新について説明する。図９に示すように、まず、電源を投入してクライアントを起動させる（Ｓ１００）と、そのＯＳが起動する（Ｓ１１０）。起動したＯＳの制御により、ネットワーク接続や各種ソフトウエアによるサービスが起動し（Ｓ１２０）、ネットワークを介したデータの授受が可能となる。そして、クライアントは、セキュリティソフトウエアの実行によりポリシファイルの更新機能が起動し（Ｓ１３０）、ネットワークを介して管理端末から、前述したポリシファイルの更新を受ける。す

なわち、クライアントは、管理端末からポリシファイルの最新バージョンを受信する（Ｓ１３０）。そして、クライアントは、ユーザの操作入力に応じた各種の処理が実行可能となる（Ｓ１４０）。

【０００９】

【非特許文献１】

村瀬康治著「入門ＭＳ－ＤＯＳ　改訂新版」株式会社アスキー出版、１９９１年８月１１日ｐ．６３－６４

【００１０】

【非特許文献２】

村瀬康治著「入門ＭＳ－ＤＯＳ　改訂新版」株式会社アスキー出版、１９９１年８月１１日ｐ．１３１－１３２

【００１１】

【発明が解決しようとする課題】

前述した従来の技術にあっては、クライアントに付帯するストレージにポリシファイルが格納されている。このため、クライアントの動作が停止中では、当然ながら、ポリシファイルを更新することができない。このため、ポリシファイルを更新するまでの間、アクセス制御やウイルス対策等を最新の状態で行うことができない。

【００１２】

また、図９のフローチャートで示したように、起動後にクライアントのポリシファイルが更新されるため、起動してからアップデートされるまでの間、古いバージョンのセキュリティ情報で運用されることになる。この間、アクセス制御やウイルス対策等を最新の状態で行うことができない。特に、ネットワーク感染型のウイルスは、ネットワークに接続されている機器に対して攻撃する。このため、起動してからアップデートされるまでの間、クライアントは常時攻撃を受けうる無防備な状態となってしまう。

【００１３】

さらに、ポリシの更新作業に関し、複数あるクライアントそれぞれについて、ポリシの更新作業を実施しなければならず、各クライアントすべての管理負担が

膨大となる。

【００１４】

【課題を解決するための手段】

本発明が提供する主たる技術では、クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新する。

本発明の他の特徴については、本明細書及び添付図面の記載により明らかにする。

【００１５】

【発明の実施の形態】

＝＝＝＝＝発明の概要＝＝＝＝＝

本明細書及び添付図面の記載により、少なくとも次の事項が明らかとなる。

本実施の形態に係る、セキュリティに関する情報を更新する方法では、クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、

前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新するステップを備える。

前記クライアントはローカルなディスク装置を有しないこととできる。

前記サーバは管理端末とネットワークを通じて接続され、前記セキュリティ情報を更新するステップでは、前記管理端末が、前記セキュリティ情報を更新することとできる。

前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることとできる。

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることとできる。

前記クライアントが前記セキュリティ情報を参照することとできる。

前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むこととできる。

【００１６】

本実施の形態に係るクライアントでは、サーバにネットワークを通じて接続するのであって、前記クライアントが管理する記憶装置を前記サーバに備え、前記記憶装置には、前記セキュリティ情報が格納されており、前記セキュリティ情報は更新され、前記セキュリティ情報を参照する。

前記クライアントはローカルなディスク装置を有しないこととできる。

前記サーバは管理端末とネットワークを通じて接続され、前記管理端末が、前記セキュリティ情報を更新することとできる。

前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることとできる。

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることとできる。

前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むこととできる。

【００１７】

本実施の形態に係るサーバでは、クライアントとネットワークを通じて接続されるのであって、前記クライアントによって管理される記憶装置を備え、前記記憶装置には、前記セキュリティ情報が格納され、前記セキュリティ情報は更新される。

前記クライアントはローカルなディスク装置を有しないこととできる。

前記サーバは管理端末とネットワークを通じて接続され、前記管理端末が、前記セキュリティ情報を更新することとできる。

前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることとできる。

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることとできる。

前記セキュリティ情報は、前記クライアントにより、参照されることとできる。

前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むこととできる。

【００１８】

本実施の形態に係る管理端末では、クライアントによって管理される記憶装置を備えたサーバとネットワークを通じて接続されるのであって、前記サーバの前記記憶装置には前記セキュリティ情報が格納されており、前記セキュリティ情報を更新する。

【００１９】

＝＝＝＝＝実施例＝＝＝＝＝

クライアントは、ローカルのハードディスク装置を備えない、いわゆるディスクレスのコンピュータで構成される。本実施例では、このクライアントをディスクレスクライアントと称する。

【００２０】

図１に示すように、一又は複数台のディスクレスクライアント１００がネットワークを介してストレージサーバと称するサーバ２００に接続する。このサーバ２００には、ネットワークを介して管理端末３００（図中では管理用計算機）が接続される。なお、この管理端末３００の機能をサーバ２００が備えることで、管理端末３００を省略してもよい。

【００２１】

ディスクレスクライアント１００は、従来同様、ＣＰＵ１１０、メモリ１２０及びネットワークインタフェース１３０を装備している。メモリ１２０には、ＯＳ１２１、セキュリティソフトウエア１２２、アプリケーションプログラム１２３、及びネットワークストレージドライバ１２４がサーバ２００から読み出されて展開される。また、ディスクレスクライアント１００は、その記憶装置の機能をディスクイメージ２２０としてサーバ２００に持たせている。

すなわち、ディスクレスクライアント１００は、ローカルなディスク装置を有さず、サーバ２００のハードディスク装置（ストレージ，記憶装置）がマウントされている。ディスクレスクライアント１００のネットワークストレージドライバ１２４が、ネットワーク経由でマウントされたサーバ２００のディスクを制御する。

【００２２】

サーバ２００は、ネットワークインタフェース２１０及びＣＰＵ２２０を備えるとともに、各ディスクレスクライアント１００が管理するハードディスク装置を多数備える。このサーバ２００は、例えばＲＡＩＤ（Redundant Array of Inexpensive Disks）方式で運用してもよい。ハードディスク装置には、ディスクレスクライアント１００が使用するディスクイメージ２３０が格納される。このディスクイメージ２３０は、各ディスクレスクライアント１００毎に存在する。このディスクイメージ２３０とは、前述した図７に示す従来のクライアントのストレージ（ハードディスク装置）に格納されたものと同じファイル群である。

すなわち、ディスクレスクライアント１００が使用するディスクイメージ２３０は、ＯＳの構成に関するＯＳ構成ファイル群２３１、ポリシファイル群２３２及びその他のファイル群２３３である。これらファイル群２３１乃至２３３には、前述した従来の技術と同様のセキュリティ情報が含まれる。

すなわち、ポリシファイル群２３２は、前述した、アクセス制御情報、ウイルスパターンファイル、及びシグネチャファイル等で構成される。その他のファイル群２３３は、セキュリティソフトウエア１２２、アプリケーションプログラム１２３、及びソフトウエアやプログラムが使用するデータファイル、ネットワークストレージドライバ１２４を含む。加えて、その他のファイル群２３３には、ファイルの属性やファイルアロケーションテーブル等、図２乃至図４に示すように様々なファイルの管理情報がファイルシステムとして含まれる。

【００２３】

管理端末３００は、ＣＰＵ３１０、メモリ３３０、ネットワークインタフェース３２０、及びハードディスク装置で構成されるストレージ３４０を備えている。メモリ３３０には、ＯＳ３３１、管理用ソフトウエア３３２及びアプリケーシ

ョンプログラム３３３が展開される。ストレージ３４０には、ＯＳ、管理ソフトウエア及びアプリケーションプログラム及びデータファイル等、各種ファイル群３４１乃至３４３が格納されている。管理用ソフトウエア３３２が管理ソフトウエアファイル群３４２を用いて、サーバ２００のディスクイメージ２３０における各種ファイル群３４１乃至３４３の内容、すなわち、セキュリティ情報を更新して最新のバージョンとする。

【００２４】

具体的なポリシのアップデート手順を図５に示す。図１に示すように、従来と異なり、ディスクレスクライアント１００が使用するポリシは、サーバ２００が保持する各種ファイル群２３１乃至２３３に含まれる。そして、随時、サーバ２００がポリシのアップデート機能を起動し（Ｓ２００）、管理端末３００から適宜各種ファイル群２３１乃至２３３の最新版を受け取り、ポリシのアップデートを完了する（Ｓ２１０）。このことで、サーバ２００が接続するネットワーク全体において、ファイルの属性やユーザＩＤをはじめ、各種ウイルス対策等のポリシのアップデートが行われる。このことで、不正アクセスやウイルスの侵入や攻撃等に対し、最新のセキュリティが確保される。

【００２５】

このポリシのアップデートの完了後に、ディスクレスクライアント１００が起動する（Ｓ２２０）。詳しくは、ディスクレスクライアント１００が電源投入されるとＩＰＬ（Initial Program Loader）が起動される。ＩＰＬの作用によりネットワークを通じてサーバ２０のディスクイメージ２３０から基本ＯＳが呼び出され、ディスクレスクライアント１００のメモリ１２０に基本ＯＳが展開される。展開された基本ＯＳが動作を開始（Ｓ２３０）することにより、ディスクレスクライアント１００はコンピュータとしての動作を開始する。

【００２６】

起動したＯＳの制御により、ディスクレスクライアント１００は、ネットワーク接続や各種ソフトウエアによるサービスが起動し（Ｓ２４０）、ネットワークを介したデータの授受が可能となる。動作を開始したディスクレスクライアント１００は、ユーザのＩＤ（ユーザ名）やパスワード等の認証情報の入力を受け付

けると、サーバ２００のディスクイメージ２３０内のファイル群２３１，２３２内に登録された認証情報と照合する。照合の結果、グループＩＤ（グループ名）も含めた認証情報の正当性が確認されると、ユーザによるクライアントの使用を可能とする。

【００２７】

ディスクレスクライアント１００でアプリケーションプログラムが動作する場合において、セキュリティソフトウエア１２２によるセキュリティを高める追加のアクセス制御について説明する。セキュリティソフトウエア１２２は、前述したアクセス制御機能を強化すべく、ＯＳに追加するソフトウエアである。このセキュリティソフトウエア１２２は、ポリシファイルに記述されたアクセス制御情報に基づき、よりセキュリティを高める緻密なアクセス制御を行う。このポリシファイルには、アプリケーションプログラム等が使用するファイルに対するアクセスを許可する条件として、ユーザやアプリケーション及び時間帯等の詳細な属性が特定されている。

【００２８】

すなわち、図６のフローチャートに示すように、ＯＳの制御の下では、図１のアプリケーションプログラム１２３が、サーバ２００のディスクイメージ２３０内のファイルに対してアクセスを要求すると（Ｓ３１０）、セキュリティソフトウエア１２２による追加のファイルアクセス制御が機能する（Ｓ３１１）。このファイルアクセス制御により、サーバ２００のディスクイメージ２３０内のポリシファイル２３２を参照し、アクセスが要求されたファイルについて、そのポリシを確認する（Ｓ３１２）。このポリシとしては、各ファイルに関し、その属性、アクセスを許可するユーザＩＤやアプリケーションを特定する情報である。このポリシの確認の結果、アプリケーションによるファイルアクセスが許可されると、次にＯＳによるファイルアクセス制御が機能する。このＯＳのファイルアクセス制御により、アクセスが要求されたファイルについて、そのファイルシステムを参照し、図４に示すファイル属性を確認する（Ｓ３１３）。この確認の結果、ユーザＩＤが一致する等でアクセスが許可されると、ネットワークストレージドライバ１２４がネットワークインタフェース１３０を介し、サーバ２００のデ

ィスクイメージ２３０内のファイルにアクセスする（Ｓ３１４→Ｓ３１５→Ｓ３１６）。

【００２９】

以上、本発明の実施の形態について、その実施の形態に基づき具体的に説明したが、これに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

【００３０】

本発明の実施の形態にあっては次の効果を奏する。

ディスクレスのクライアントが管理して使用するディスクは、ネットワーク上のサーバにマウントされている。加えて、このサーバにマウントされたディスクには、ポリシ（セキュリティポリシ）やファイルを含むクライアントのディスクイメージが格納されている。そして、このディスクイメージにおけるポリシの更新については、管理端末が行う。

【００３１】

このため、クライアントの動作停止の有無に関わらず、随時、ポリシ（セキュリティ情報）を更新することができる。したがって、停止中のクライアントが起動した時点では、既にポリシの更新が完了している。このため、クライアントは常時更新されたポリシに則って運用される。

【００３２】

複数のクライアントが一つのサーバにディスクをマウントする場合でも、サーバのポリシを更新するだけで済む。例えば、管理端末を介してサーバのポリシを更新する。すなわち、従来のように、各クライアントそれぞれについて、ポリシの更新作業を実施する必要がなく、各クライアントの管理負担を大幅に軽減することができる。

【００３３】

【発明の効果】

クライアントが動作停止中でも、セキュリティ情報を更新することができる。

【図面の簡単な説明】

【図１】　本発明に係る一実施例を示すシステムブロック図である。

【図２】　本発明に係る一実施例におけるファイル属性を示す図表である。

【図３】　本発明に係る一実施例におけるアロケーションテーブルを示す図表である。

【図４】　本発明に係る一実施例におけるクラスタの構造を示す図表である。

【図５】　本発明に係る一実施例におけるポリシのアップデート手順に示すフローチャートである。

【図６】　本発明に係る一実施例におけるファイルの追加的なアクセス制御を示すフローチャートである。

【図７】　本発明に係る一実施例におけるクライアントの構成を示すブロック図である。

【図８】　従来のクライアントによるファイルに対するアクセスの制御を示すフローチャートである。

【図９】　従来のクライアントによるポリシファイルの更新を示すフローチャートである。

【符号の説明】

１００　ディスクレスクライアント
１１０　ＣＰＵ
１２０　メモリ
１２１　ＯＳ
１２２　セキュリティソフトウエア
１２３　アプリケーションプログラム
１２４　ネットワークストレージドライバ
１３０　ネットワークインタフェース
２００　サーバ
２１０　ネットワークインタフェース
２２０　ＣＰＵ
２３０　ディスクイメージ
２３１　ＯＳ構成ファイル群

２３２　ポリシファイル群

２３３　その他のファイル群

３００　管理端末

３１０　ＣＰＵ

３２０　ネットワークインタフェース

３３０　メモリ

３３１　ＯＳ

３３２　管理用ソフトウエア

３３３　アプリケーションプログラム

３４０　ストレージ

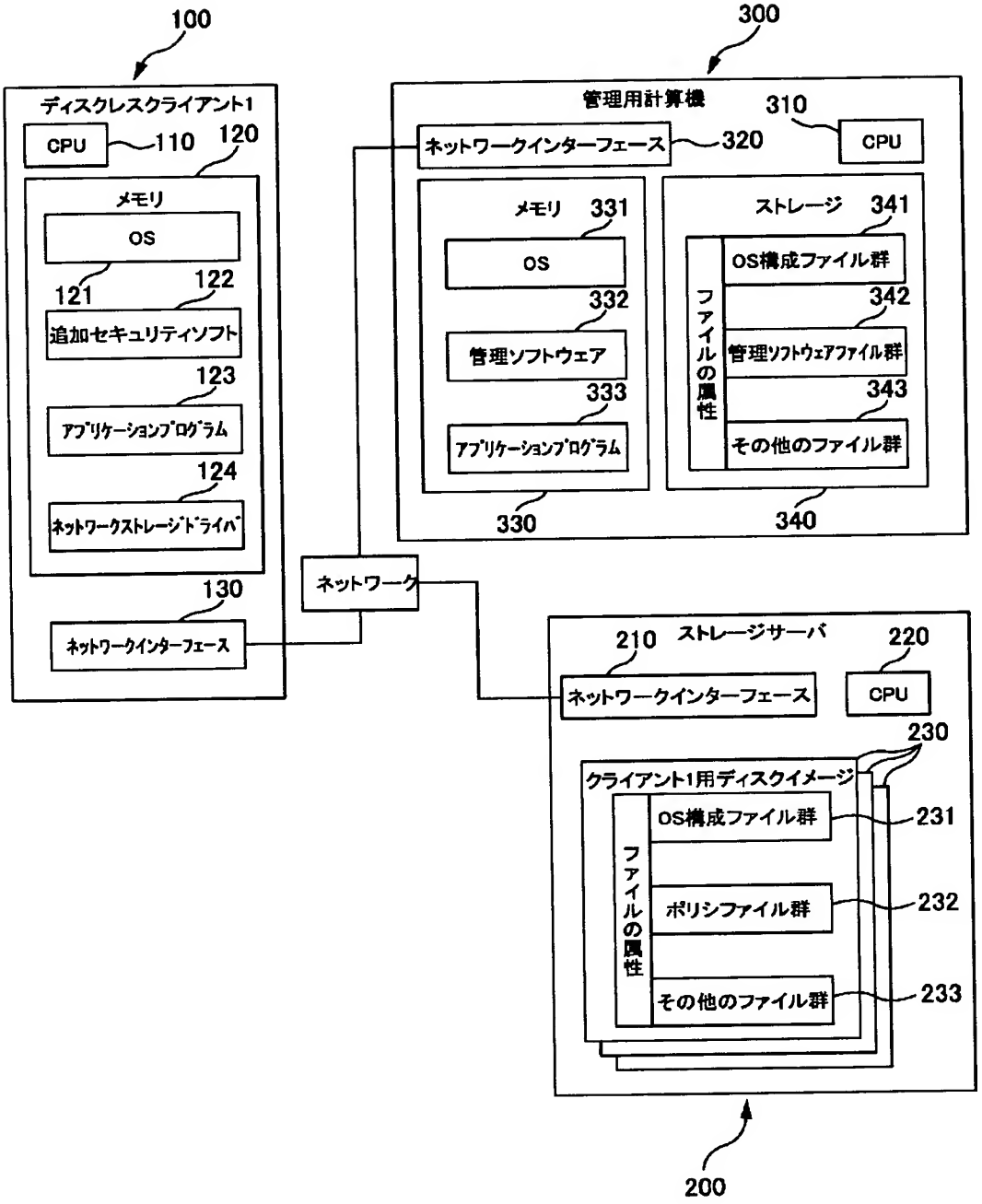
３４１　ＯＳ構成ファイル群

３４２　管理ソフトウエアファイル群

３４３　その他のファイル群

【書類名】　　図面

【図１】


100
ディスクレスクライアント1
CPU
110
120
メモリ
OS
121
122
追加セキュリティソフト
123
アプリケーションプログラム
124
ネットワークストレージドライバ
130
ネットワークインターフェース
300
管理用計算機
310
CPU
ネットワークインターフェース
320
メモリ
331
OS
332
管理ソフトウェア
333
アプリケーションプログラム
330
ストレージ
341
OS構成ファイル群
342
管理ソフトウェアファイル群
343
その他のファイル群
ファイルの属性
340
ネットワーク
210
ストレージサーバ
220
ネットワークインターフェース
CPU
230
クライアント1用ディスクイメージ
OS構成ファイル群
231
ポリシファイル群
232
その他のファイル群
233
ファイルの属性
200

【図２】

ファイル属性

		日付					所有者			グループ			外部			
ファイル名	パス名	作成	変更	参照	所有者名	グループ名	読	書	実行	読	書	実行	読	書	実行	AT
test.txt	¥tmp¥	2000/2/3	2001/3/4	2001/4/5	usera	groupa	可	可	否	可	否	否	可	否	否	15
foo.doc	¥sys¥	2002/1/1	2002/1/1	2002/5/6	root	root	可	否	否	否	否	否	否	否	否	23
bar.exe	¥bin¥	2000/2/3/	2000/2/3/	2002/5/6	deamon	deamon	可	可	可	可	否	可	可	否	可	48
…																

【図３】

アロケーションテーブル(4～8バイト/マス)

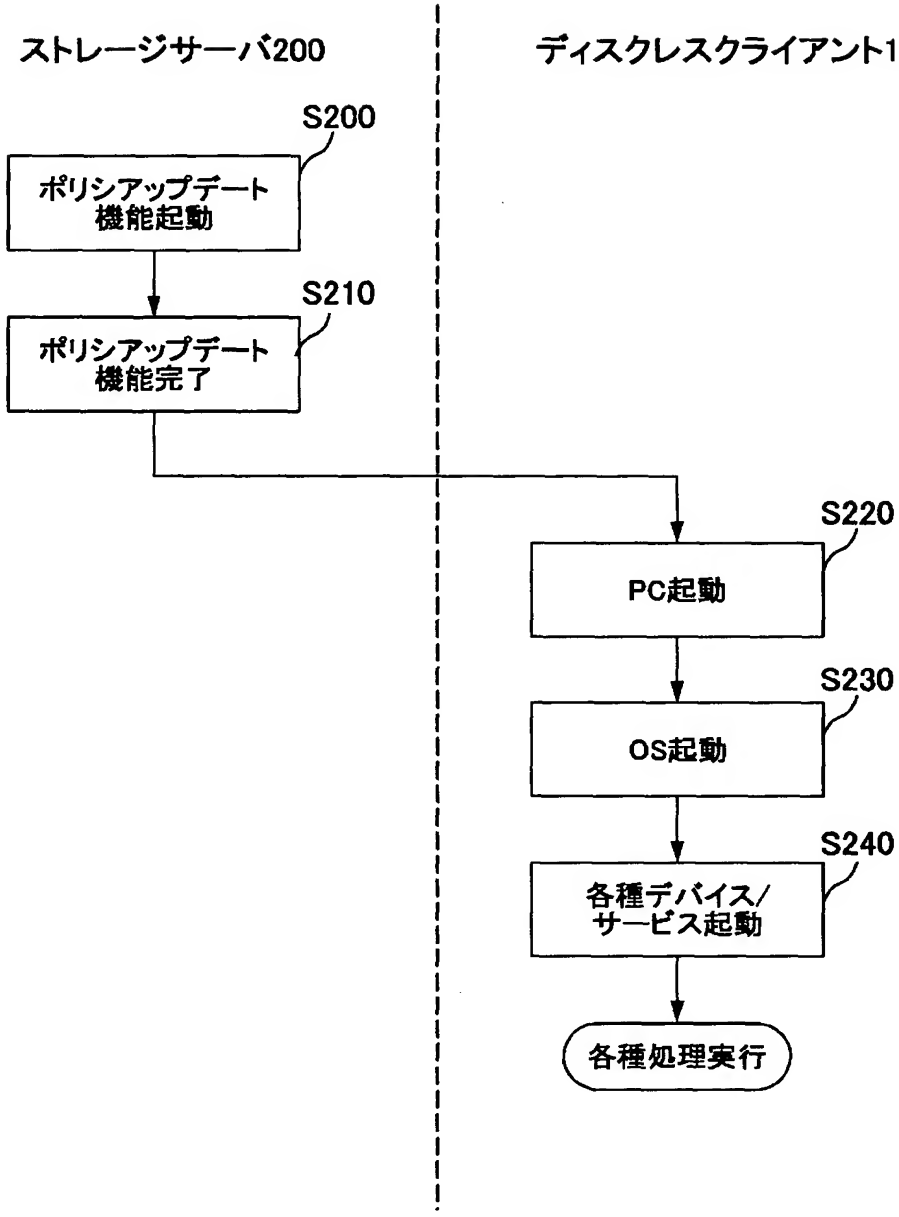
	0	1	2	3	4	5	6	7	8	9
0			5			8			63	
10						16	17	18	19	20
20	0			24	25	30				
30	31	32	33	0						
40									2	
50										
60				67				0		
…										

【図４】

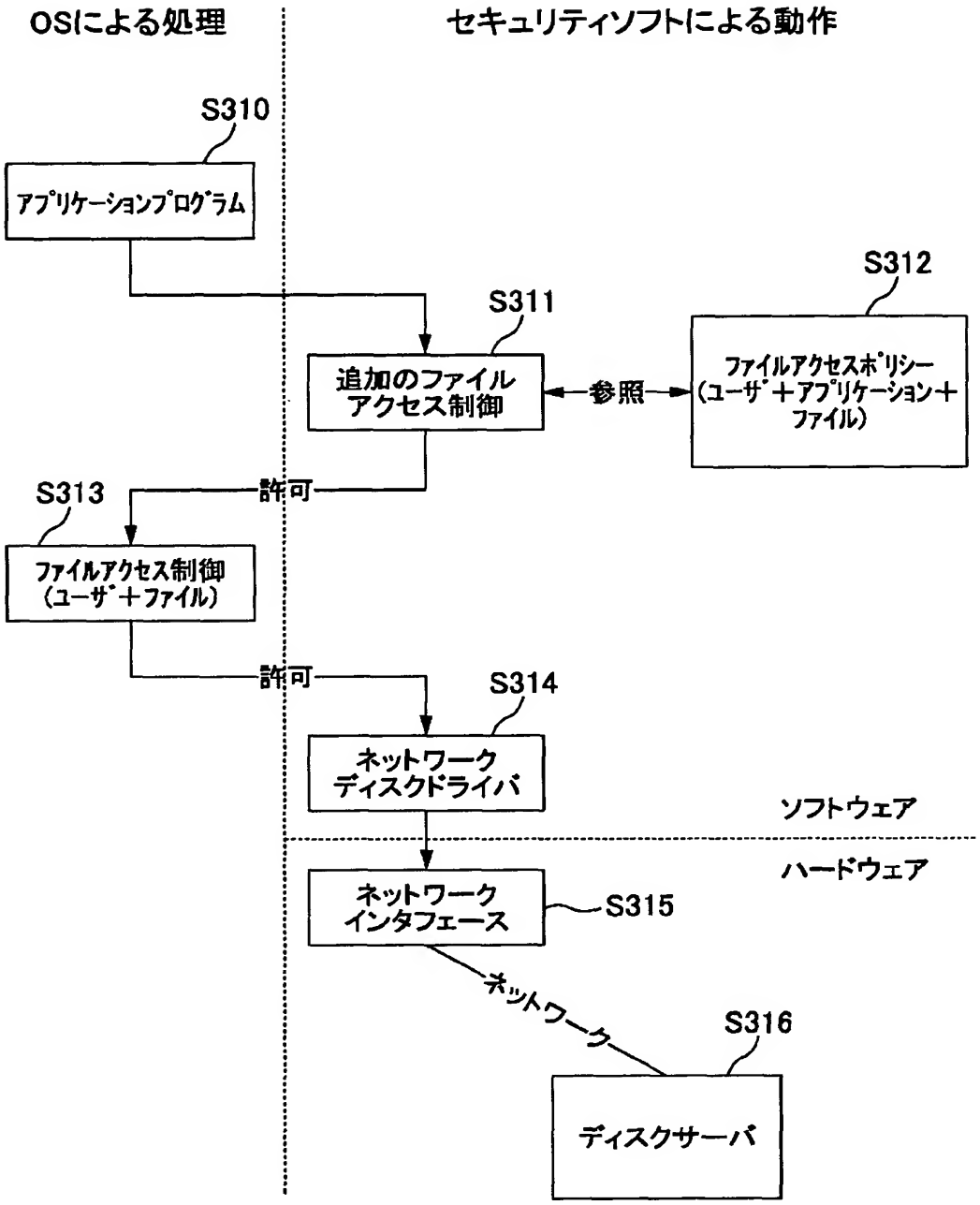
クラスタ(4～32バイト/マス)

	0	1	2	3	4	5	6	7	8	9
0			*			*			*	
10						*	*	*	*	*
20	*			*	*	*				
30	*	*	*	*						
40									*	
50										
60				*				*		
…										

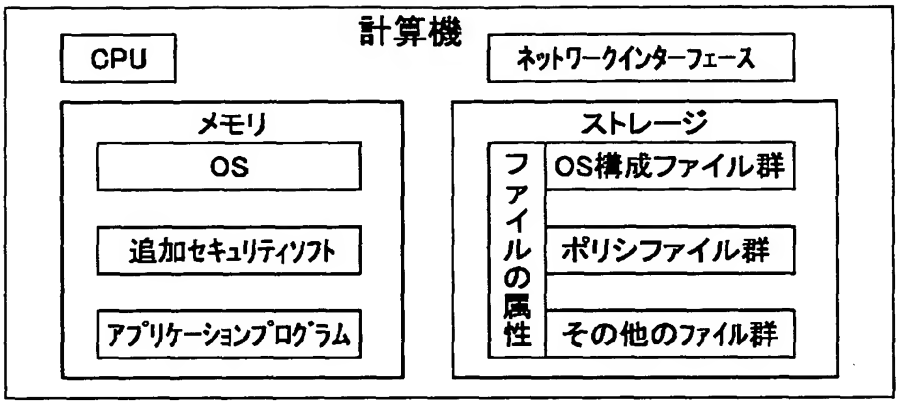
【図５】


ストレージサーバ200
ディスクレスクライアント100
S200
ポリシアップデート
機能起動
S210
ポリシアップデート
機能完了
S220
PC起動
S230
OS起動
S240
各種デバイス/
サービス起動
各種処理実行

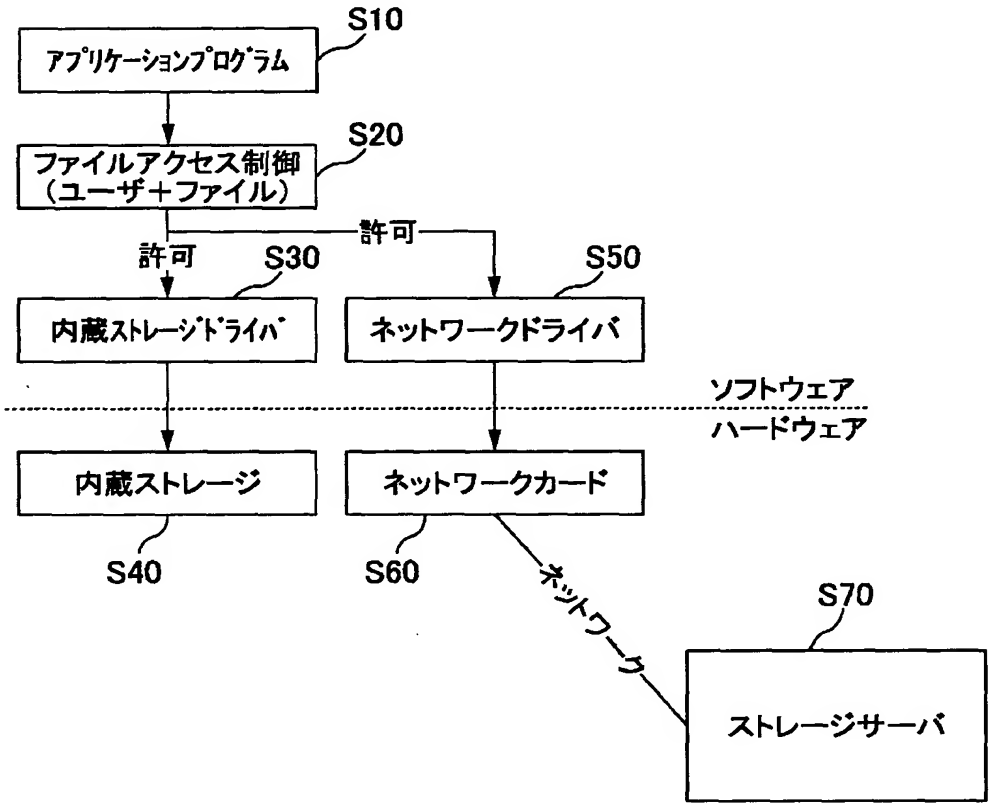
【図６】


OSによる処理
セキュリティソフトによる動作
S310
アプリケーションプログラム
S311
追加のファイル
アクセス制御
参照
S312
ファイルアクセスポリシー
(ユーザ＋アプリケーション＋
ファイル)
S313
許可
ファイルアクセス制御
(ユーザ＋ファイル)
許可
S314
ネットワーク
ディスクドライバ
ソフトウェア
ハードウェア
ネットワーク
インタフェース
S315
ネットワーク
S316
ディスクサーバ

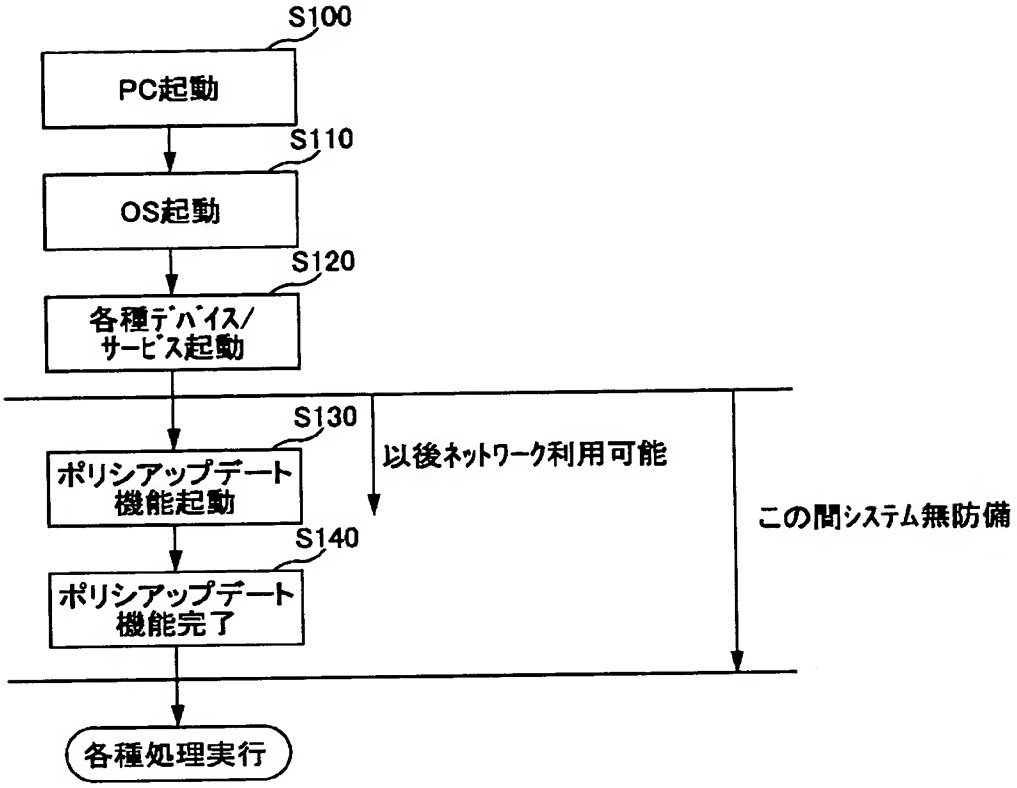
【図７】


計算機
CPU
ネットワークインターフェース
メモリ
OS
追加セキュリティソフト
アプリケーションプログラム
ストレージ
ファイルの属性
OS構成ファイル群
ポリシファイル群
その他のファイル群

【図８】


S10
アプリケーションプログラム
S20
ファイルアクセス制御
（ユーザ＋ファイル）
許可
許可
S30
S50
内蔵ストレージドライバ
ネットワークドライバ
ソフトウェア
ハードウェア
内蔵ストレージ
ネットワークカード
S40
S60
ネットワーク
S70
ストレージサーバ

【図９】


S100
PC起動
S110
OS起動
S120
各種ﾃﾞﾊﾞｲｽ/
ｻｰﾋﾞｽ起動
S130
ポリシアップデート
機能起動
以後ネットワーク利用可能
S140
ポリシアップデート
機能完了
この間システム無防備
各種処理実行

【書類名】　　要約書

【要約】

【解決手段】　クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新する。

【選択図】　　図１

出証特２００３－３００７９６２

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
　［変更理由］　新規登録
　　住　所　東京都千代田区神田駿河台４丁目６番地
　　氏　名　株式会社日立製作所